KEJAHATAN DI BIDANG KUMPUTER "*CYBERCRIME*" DAN PENANGGULANGANNYA

Ruslan Abdul Gani[1]

Abstract

Era of globalization and information technology had an influence on the emergence of various forms of crimes that are new. The emergence of a new crime (cyber crime) is a phenomenon that requires quick and accurate response.

The term cyber crime is currently refers to an act of crime associated with the virtual world (cyberspace) and crimes using computers. In general we can say the field of computer crime in general can be defined as the use of computers illegally. Or include all offenses relating to information, information system itself.

Keyword : Technology, Cybercrime

PENDAHULUAN

Istilah komputer berasal dari bahasa Inggris "*computer*" yang kata dasarnya to compute yang berarti menghitung. Istilah computer yang semula artinya perhitungan, kemudian berkembembang lebih luas karena istilah kalkulator khusus dipakai untuk mesin hitung, yang asal katanya *to calculate* (Andi Hamzah: 1983).

Istilah komputer (computer) yang semula dipakai untuk alat menghitung suara pemilihan Presiden (voting) itu berkembang terus sesuai dengan kemajuan teknologi elektronik yang canggih.

Ada yang melukiskan komputer itu secara sederhana Serangkaian atau kumpulan mesin elektronik yang bekerja bersama-sama dan dapat melakukan rentetan atau rangkaian pekerjaan secara otomatis melalui instruksi atau program yang diberikan kepadanya (Lembaga Pendd Kom Indonesia Amerika).

Dari pendapat tersebut di atas memberikan gambaran kepada kita bahwa komputer ini memiliki beberapa cirri sebagai berikut:

1. Komputer itu merupakan suatu system, yaitu serangkaian atau sekelompok peralatan yang bekerja bersama-sama secara elektronis.
2. Komputer mempunyai suatu alat penyimpan data dan program yang disebut dengan stroge atau memory computer.
3. Komputer itu bekerja di bawah control operating systems atau system operasi dan melaksanakan tugas berdasarkan instruksi – instruksi yang disebut program.

Adapun yang dimaksud dengan *operating system* adalah: "Sekumpulan program atau instruksi yang dibuat oleh pihak komputer dengan memperhatikan bentuk serta cara kerja dari hardware yang mereka miliki".

Jadi operating system adalah merupakan silent parter pada waktu kita memakai kumputer, dimana operating system merupakan program yang bisa bertindak sebagai penyelaras atau jembatan kerja antara hardware komputer dengan segala macam *system software* yang ada.

Sebagai system operasi, operating system ini berfungsi untuk mengatur dan mengontrol sumber daya yang ada; baik dari hardware yang berupa komputer, *Central processing Unit* (CPU) dan memory storage serta software komputer yang berupa program-program komputer yang dibuat oleh programmer. Dengan adanya operating syster ini pihak pemakai komputer dapat memamfaatkan komputer yang ada semaksimal mungkin.

Walaupun komputer untuk saat ini dikategorikan peralatan yang canggih, namun dibalik kecanggihannya tersebut tidak dilengkapi dengan proteksi untuk melindungi perbuatan-perbuatan yang merugikan para pencipta atau orang lain. Sehingga tidak heran untuk saat ini timbul kejahatan di bidang kumputer yang dikenal dengan istilah "*Cybercrime*"

Cybercrime merupakan salah satu bentuk atau dimensi baru dari kejahatan masa kini yang mendapat perhatian luas di dunia internasional. Volodymyr Golubev menyebutkan sebagai:

"*the new form of antisocial behavior*".) Beberapa julukan/sebutan lainnya yang "cukup keren" diberikan kepada jenis kejahatan baru ini di dalam berbagai tulisan, antara lain, sebagai "kejahatan dunia maya" ("*cyberspace/virtual space offence*"), dimensi dari "*hitech crime*", dimensi baru dari "*transnational crime*", dan dimensi baru dari "*white collar crime*". Bahkan

[1] Dosen Fak. Hukum Universitas Batanghari

dapat dikatakan sebagai dimensi baru dari "*environmental crime*" (Donn B Parker : 1976).

Cybercrime (selanjutnya disingkat "CC") merupakan salah satu sisi gelap dari kemajuan teknologi yang mempunyai dampak negatif sangat luas bagi seluruh bidang kehidupan modern saat ini. Kekhawatiran demikian terungkap pula dalam makalah "*Cybercrime*" yang disampaikan oleh ITAC *(Information Technology Association of Canad*a) pada "*International Information Industry Congress* (IIIC) 2000 Millenium Congress" di Quebec pada tanggal 19 September 2000, yang menyatakan bahwa "*Cybercrime is a real and growing threat to economic and social development around the word. Information technology touches every aspect of human life and so can electronically enabled crime*."[)] Sehubungan dengan kekhawatiran akan ancaman / bahaya CC ini, karena berkaitan erat dengan *economic crimes* dan *organized crime* (terutama untuk tujuan *money laundering*), maka Kongres PBB mengenai "*The Prevention of Crime and the Treatment of Offenders*" (yang diselenggarakan tiap 5 tahun) telah pula membahas ini. Sudah dua kali masalah CC ini diagendakan, yaitu pada Kongres VIII/1990 di Havana dan pada Kongres X/2000 di Wina.

Memerhatikan perkembangan dua Kongres International di atas (yaitu Kongres mengenai"Industri Informasi Internasional" dan Kongres PBB mengenai "Pencegahan Kejahatan"), maka wajar Indonesia pun seyogianya melakukan antisipasi terhadap upaya penanggulangan "CC" ini.

PERMASALAHAN

Untuk menghidari agar makalah ini pembahasannya tidak terlalu luas dan menyimpang dari pokok permasalahannya yang ingin di bahas, maka penulis perlu membatasi permasalahannya yang hanya menyangkut : Jenis Penyalahgunaan Komputer yang bagaimana dikategorikan suatu kejahatan Cybercrime.

PEMBAHASAN

1. Jenis Penyalahgunaan Komputer yang dikategorikan suatu kejahatan *Cybercrime*.

Komputer sebagai barang berwujud dan berharga sudah tentu dapat dapat menjadi objek kejahatan. Kejahatan di sini ialah kejahatan biasa atau konvensional, seperti pencurian, perusakan, sabotase, pembukaan rahasia dan sebagainya.

Jadi di dalam pengertian ini dapat dibagi 2, computer dapat menjadi objek, bukan media atau alat untuk melakukan kejahatan. Misalnya perbuatan mencuri perangkat komputer, merusak komputer seperti membongkar, memecah, menghancurkan dan sebagainya. Bukan ini yang dimaksud dengan penyalahgunaan komputer.

Penyalahgunaan komputer, yaitu komputer menjadi alat atau media untuk melakukan kejahatan, seperti mencuri uang melalui komputer, menggelapkan uang, korupsi, membocorkan rahasia perusahaan, rahasia Negara, mata-mata dan sebagainya.

Menurut Donn B. Parker di dalam bukunya Andi Hamzah dijelaskan adapun yang dimaksud dengan Penyalahgunaan Komputer adalah:

Sebagai suatu kejadian yang berhubungan dengan teknologi komputer yang seorang korban menderita atau akan telah menderita kerugian dan seorang pelaku dengan sengaja memperoleh keuntungan atau akan telah memperoleh keuntungan (Andi Hamzah : 1983).

Keuntungan di sini dalam arti luas, termasuk memperoleh manfaat. Kalau kita perhatikan defenisi Parker tentang Penyalahgunaan Komputer ini, maka perbuatan yang tidak menyebabkan pembuat mendapat manfaat, tidak termasuk penyalahgunaan komputer (*computer abuse*), seperti perusakan, sabotase, yang hanya karena balas dendam.

Negara Belanda melalui Komisi Franken yaitu suatu komisi yang dibentuk untuk menguji dan menyusun delik komputer di dalam KUHP, mengemukakan bahwa : Kejahatan komputer (*Computer crime naliteit*) selalu disosialisasikan dengan perilaku yang merugikan yang menyangkut system pengolahan data.

Jadi, di sini meliputi kejahatan komputer pada umumnya. Terdiri dari Dua unsur, yaitu tingkah laku yang merugikan (orang lain) dan sistem pengolahan data.

Sehubungan dengan penyalahgunaan komputer tersebut di atas, muncul istilah-istilah terhadap perbuatan-perbuatan yang termasuk kejahatan dibidang komputer *(Cybercrime)* antara lain:

1. *Joycomputing*:

Yaitu pencurian waktu operasi komputer yang disebut di dalam bahasa Belanda *tijd diefstal*.

2. *Hacking*:

Yaitu memasuki atau merusak atau mengakses secara tidak sah, yang disebut di dalam bahasa Belanda, *onbevoegd zich toegang verschaffen.*

3. *The Trojan horse*:

Yaitu mengubah, menambah, menghapus data, yang secara umum disebut di dalam bahasa belanda data manipulatie (*gegevens manipulatie*).

4. *Data leakage*:

Yaitu pembocoran data rahasia ke luar perusahaan (instansi) yang disebut di dalam bahasa Belanda *onbevoegd kennis nemen van gegevens* (mengetahui data secara tidak berwenang).

5. *Data diddling:*

Yaitu mengubah data yang sah menjadi tidak sah atau mengubah input atau output, yang termasuk pemalsuan data, yang disebut dalam bahasa Belanda *Vervalsen*.

6. *To frustrate data communication*:

Yaitu menggagalkan atau menyia-nyiakan data, yang disebut di dalam bahasa Belanda *verijdeling data communicatie*.

7. *Software piracy*:

Yaitu pembajakan hak cipta terhadap perangkat lunak komputer (*software*) yang disebut di dalam bahasa Belanda *software piraterij (*Al. Wisnubroto: 1999*)*.

Kendala yang dihadapi sehubungan dengan penyidikan kejahatan dibidang komputer (Cybercrime) menurut Andi Hamzah pada padasarnya ada dua macam yaitu:

1. Kendala yang Non yuridis.
2. Kendala yuridis.

Yang dikatakan kendala Non Yuridis di sini, ialah pertama masalanya orang melapor kejahatan, terutama kejahatan komputer.

Kejahatan komputer lebih besar lagi karena :

a. Suatu perusahaan yang melaporkan terjadi kejahatan komputer di dalam perusahaannya, akan merugikan nama perusahaa itu sendiri.
b. Sekiranya pimpinan suatu perusahaan tidak tahu cara bagaimana mengoreksi suatu penyalahgunaan berakibat sering suatu kejadian berulang-ulang terjadi tetapi tidak tahu cara bagaimana menghentikan kejahatan tersebut.
c. Sering pimpinan perusahaan berusaha agar sedikit mungkin orang luar tahu terjadinya kejahatan, dan sering takut balas dendam dari pelaku yang menyabotase, sehingga ia hanya dipindah, dan dikenakan pelanggaran administrasi.

Sedangkan kendala yuridis yang timbul dari kejahatan komputer antara lain:

a. Masalah Pembuktian.
b. Penyelesaian bentuk-bentuk kejahatan yang terjadi dan rumusan delik yang tersedia.
c. Khusus untuk Indonesia, belum ada rumusan delik baru mengenai kejahatan komputer, jadi masih memakai rumusan lama yang serba kurang , sehingga harus penafsiran ekstensif.

Dalam rangka upaya menaggulangi *Cybercrime* itu Resolusi Kongres PBB VIII/1990 mengenai "*Computer – related crime* mengajukan beberapa kebijakan antara lain sebagai berikut (United Nations, Eight Un Congress on the Prevention of Crime and the Treatment of Offenders, Report, :1991)

a. Mengimbau Negara anggota untuk mengintensifkan upaya-upaya penaggulangan penyalahgunakan komputer yang lebih efektif dengan mempertimbangkan langkah-langkah sebagai berikut:
    1. Melakukan modernisasi hukum pidana materiil dan hukum acara pidana;
    2. Mengembangkan tindakan-tindakan pencegahan dan pengamanan komputer;
    3. Melakukan langkah-langkah untuk membuat peka (sensitif) warga masyarakat, aparat pengadilan, dan penegak hukum, terhadap pentingnya pencegahan kejahatan yang berhubungan dengan komputer (untuk selanjutnya dalam kutipan ini disingkat dengan inisial "CC");
    4. Melakukan upaya-upaya pelatihan (training) bagi para hakim, pejabat, dan aparat penegak hukum mengenai kejahatan ekonomi dan "CC";
    5. Memperluas "rules of ethics" dalam penggunaan komputer dan mengajarkannya melalui kurikulum informatika;

6. Mengadopsi kebijakan perlindungan korban "CC" sesuai dengan Deklarasi PBB mengenai korban, dan mengambil langkah-langkah untuk mendorong korban melaporkan adanya "CC".

b. Mengimbau Negara anggota menigkatkan kegiatan internasional dalam upaya penaggulangan "CC";
c. Merekomendasikan kepada Komite Pengendalian dan pencegahan Kejahatan (*Committee on Crime Prevention and Control*) PBB untuk;
   - menyebarluaskan pedoman dan standar untuk membantu Negara anggota menghadapi "CC" di tingkat nasional, regional dan internasional;
   - mengembangkan penelitian dan analisis lebih lanjut guna menemukan cara-cara baru menghadapi problem CC di masa yang akan datang;
   - mempertimbangkan "CC" sewaktu meninjau pengimplementasian perjanjian ekstradisi dan bantuan kerja sama di bidang penanggulangan kejahatan.

Garis kebijakan penaggulanggan "CC" yang dikemukakan dalam Resolusi PBB di atas, terlihat cukup komprehensif. Tidak hanya penanggulangan melalui kebijakan "penal" (baik hukum pidana materiil maupun hukum pidana formal), tetapi juga kebijakan "non penal". Hal menarik dari kebijakan nonpenal yang dikemukakan dalam Resolusi PBB itu ialah upaya mengembangkan "pengamanan/perlindungan computer dan tindakan-tindakan pencegahan" ("computer security and prevention measures"; lihat poin a.2 di atas). Jelas hal ini terkait dengan pendekatan "techno-prevention", yaitu upaya pencegahan/penanggulangan kejahatan dengan menggunakan teknologi. Sangat disadari, bahwa "CC" yang terkait erat dengan kemajuan teknologi, tidak dapat semata-mata ditanggulangi dengan pendekatan yuridis, tetapi juga harus ditanggulangi dengan pendekatan teknologi itu sendiri. Menurut Volodymyr Golubev, banyak aspek dari kasus-kasus CC lebih merupakan akibat lemahnya perlindungan informasi dari pada diakibatkan oleh perbuatan pelaku kejahatan. Oleh karena itu, perlu di berikan lebih banyak informasi mengenai kelemahan/kerentanan dari sistem komputer dan sarana perlindungan yang efektif. Perlunya penanggulangan/pencegahan "CC" secara teknologi, diungkapkan juga oleh IIC (International Information Industry Congress) yang menyatakan;

> "*The IIIC recognizes that government action and international treaties to harmonize laws and coordinate legal procedures are key in the fight against Cybercrime, but warns that these should not be relied upon as the only instruments. Cybercrime is enabled by technology and requires a healthy reliance on technology for its solution.*"

Aspek lain yang menarik dari kebijakan "non penal" yang terungkap dari Resolusi PBB di atas, ialah perlunya "pendekatan budaya/ cultural/etik" dalam kebijakan penanggulangan "CC", yaitu membangun/mengakibatkan kepekaan warga masyarakat dan aparat penegak hukum terhadap masalah "CC" dan menyebarluaskan/mengajarkan etika penggunaan computer melalui media pendidikan (lihat poin a.3 dan a. 5 di atas). Pentingnya pendekatan budaya ini, khususnya upaya mengembangkan kode etik dan perilaku ("*codes of behavior and ethics*"), terungkap juga dalam pernyataan IIIC (International Information Industry Congress) sebagai berikut;

> "*IIIC members are also commited to participate in the developmenof codes of behaviour and ethics around computer and Internet use, and ini campaigns for the need for ethical and responsible online behaviour. Given the international reacht of Internet crime, computer and Internet users around the world must be made aware or the need for high standatrds of conduct in cyberspace*".

Upaya penanggulangan "CC" telah pula dibahas secara khusus dalam suatu lokakarya (yaitu "*Workshop on crimes related to computer networks*") yang diorganisir oleh UNAFEI selama Kongres PBB X/2000 berlangsung. (Dokumen Kongres PBB X, A/CONF.187/L.10, tgl. 16 April 2000). Lokakarya ini dibagi dalam 4 (empat) diskusi panel. Pertama, membahas tentang "*the criminology of* computer *crime*". Kedua, membahas studi kasus mengenai "*the technical and legal issues*" yang timbul dari tindakan penyidikan dan perampassan data komputer. Ketiga, membahas masalah "*the tracing of computer communication in multinational networks*". Keempat,membahas masalah "*the relationship between law*

enforcement and computer and Internet industries". Adapun kesimpulan dari lokakarya ini adalah sebagai berikut:

a. CRC (*Computer-related crime)* harus dikriminalisasikan;
b. Diperlukan hukum acara yang tepat untuk melakukan penyidikan dan penuntutan terhadap penjahat cyber *("cybercriminals*");
c. Harus ada kerja sama antara pemerintah dan industri terhadap tujuan umum pencegahan dan penanggulangan kejahatan komputer agar Internet menjadi tempat yang aman;
d. Diperlukan kerja sama internasional untuk menelusuri/mencari para penjahat di Internet;
e. PBB harus mengambil langkah/tindak lanjut yang berhubungan dengan bantuan dan kerja sama teknis dalam penanggulangan CRC.

KESIMPULAN

Berdasarkan uraian yang telah penulis kemukakan di atas dapat disimpulkan sebagai berikut:

1. Bahwa Penyalahgunaan Komputer yang dikategorikan suatu kejahatan Cybercrime, yaitu komputer menjadi alat atau media untuk melakukan kejahatan, seperti mencuri uang melalui komputer, mengelapkan uang, korupsi, membocorkan rahasia perusahaan, rahasia Negara, mata-mata dan sebagainya. Dan menurut jenisnya yang dikategorikan sebagai kejahatan komputer dikelompokkan kedalam 7 jenis yaitu:
   1. *Joycomputing*:
   2. *Hacking*:
   3. *The Trojan horse*:
   4. *Data leakage*:
   5. *Data diddling:*
   6. *To frustrate data communication*:
   7. *Software piracy*:
2. Kendala dihadapi dalam penyidikan terhadap kejahatan Cybercrime yaitu ada dua macam yaitu:
   1. Kendala yang Non yuridis.
   2. Kendala yuridis.
3. Upaya dilakukan dalam menanggulangi kejahatan Cybercrime adalah
   a. Mengimbau Negara anggota untuk mengintensifkan upaya-upaya penaggulangan penyalahgunakan komputer yang lebih efektif.
   b. Mengimbau Negara anggota menigkatkan kegiatan internasional dalam upaya penaggulangan "CC";
   c. Merekomendasikan kepada Komite Pengendalian dan pencegahan Kejahatan (*Committee on Crime Prevention and Control*) PBB untuk;
      - menyebarluaskan pedoman dan standar untuk membantu Negara anggota menghadapi "CC" di tingkat nasional, regional dan internasional;
      - mengembangkan penelitian dan analisis lebih lanjut guna menemukan cara-cara baru menghadapi problem CC di masa yang akan datang;
      - mempertimbangkan "CC" sewaktu meninjau pengimplementasian perjanjian ekstradisi dan bantuan kerja sama di bidang penanggulangan kejahatan.

DAFTAR PUSTAKA

Al. Wisnubroto, *Kebijakan Hukum Pidana dalam Penaggulangan Penyalahgunaan Komputer*, Penerbit Universitas Atmajaya Yogyakarta:1999.

Arief Bada Nawawi, *Bungga Rampai Kebijakan Hukum Pidana*, PT. Citra Aditya Bakti: 1996.

Donn B Parker, Crime by Computer, New York: Charles Scribner Sons, 1976.

Hamzah Andi, *Hukum Pidana Yang berkaitan Dengan Komputer*, Sinar Grafika Jakarta: 1993.

-------- Lembaga Pendidikan Komputer Indonesia Amerika (LPKIA) Mengenal Dunia komputer, Jakarta: 1986.